REPORT DOCUMENTATION PAGE

Form Approved
OMB NO. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
July 31, 1996

3. REPORT TYPE AND DATES COVERED
Final Technical 1/1/90 - 5/31/96

4. TITLE AND SUBTITLE
MATHEMATICAL METHODS OF COMMUNICATION SIGNAL DESIGN

5. FUNDING NUMBERS
Grant No.
N00014-90-J-1341

6. AUTHOR(S)
Dr. Solomon W. Golomb

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(ES)
University of Southern California
Department of Electrical Engineering
Communication Sciences Institute
Los Angeles, CA 90089-2565

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Dr. Marc J. Lipman
Code 1111SP
Office of Naval Research
800 N. Quincy Street
Arlington, VA 22217-5000

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

19960820 038

DTIC QUALITY INSPECTED 4

NT

12 b. DISTRIBUTION CODE

Approved for public release; distribution unlimited.

13. ABSTRACT *(Maximum 200 words)*

A brief description on each of the following major areas is included in this report.

A. Costas Arrays (and Related Radar and Sonar Arrays)

B. Zero-Sidelobe Radar

C. Generalized Barker Sequences (and Other Polyphase Sequences)

D. Simplex Codes, and Cyclic Hadamard Difference Sets

E. Legendre and Jacobi Sequences for Radar Applications

F. Minimal Spanning Rulers (so-called "Golomb Rulers") for Pulse Radar Signal Patterns

G. Other Areas Leading to Publications

14. SUBJECT TERMS
Costas Arrays, Generalized Barker Sequences, Simplex Codes, Cyclic Hadamard Difference Sets, Zero-Sidelobe Radar, Legendre and Jacobi Sequences, "Golomb Rulers".

15. NUMBER IF PAGES
10

16. PRICE CODE

17. SECURITY CLASSIFICATION OR REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

FINAL REPORT ON

ONR Grant *NOOO14-90-J-1341*

Covering the Grant Period of

January 1, 1990 to May 31, 1996

Prepared by

Professor Solomon W. Golomb
Principal Investigator
Communication Sciences Institute
University of Southern California
Los Angeles, CA 90089-2565

COMMUNICATION SCIENCES INSTITUTE
UNIVERSITY OF SOUTHERN CALIFORNIA
LOS ANGELES, CALIFORNIA 90089-2565

DR. SOLOMON W. GOLOMB
UNIVERSITY PROFESSOR

(213) 740-7333
FAX (213) 740-8729

August 8, 1996

Dr. Marc J. Lipman
Code 1111SP
Office of Naval Research
800 N. Quincy
Arlington, VA 22217-5000

Dear Dr. Lipman:

Enclosed are 3 copies of our ONR final technical report covering the period:

1 January, 1990 - 31 May, 1996

for

ONR Grant NOOO14-90-J-1341.

We include Form SF 298 relevant to this report.

Sincerely yours,

Dr. Solomon W. Golomb

Copies to: John Starcher, San Diego Regional Office (1)
DTIC, Alexandria, VA 22314 (4)
Director, NRL, Code 2627 (1)
USC Contracts & Grants (1)

I. *Technical Accomplishments*

The following topics are the major areas investigated during the period of this Grant.

A. Costas Arrays (and Related Radar and Sonar Arrays)

B. Zero-Sidelobe Radar

C. Generalized Barker Sequences (and Other Polyphase Sequences)

D. Simplex Codes, and Cyclic Hadamard Difference Sets

E. Legendre and Jacobi Sequences for Radar Applications

F. Minimal Spanning Rulers (so-called "Golomb Rulers") for Pulse Radar Signal Patterns

G. Other Areas Leading to Publications

In the next several pages, each of these topics is described briefly, and the major publications related to this research are listed.

A. *Costas Arrays*

A *Costas array of order n* is an $n \times n$ permutation matrix in which the $n(n-1)/2$ line segments connecting pairs of 1's in the matrix are distinct as vectors, i.e. no two agree in both magnitude and slope. Thus, if $a_{ij} = a_{kl} = 1$ and $a_{mn} = a_{pq} = 1$ in the matrix, with $(i, j) \neq (k, l)$, $(m, n) \neq (p, q)$, and at least three of these four ordered pairs distinct, and if $|(a_{ij}, a_{kl})|^2 = (k-i)^2 + (l-j)^2$ equals $|(a_{mn}, a_{pq})|^2 = (p-m)^2 + (q-n)^2$, then $|(l-j)/(k-i)| \neq |(q-n)/(p-m)|$.

All known general constructions for Costas arrays (see [3], [4], [5]) involve primitive roots in finite fields. The *Welch construction*, for every prime $p > 2$, gives a Costas array of order $p-1$ by setting $a_{ij} = 1$ when $j = g^i (\mathrm{mod}\ p)$, where g is a primitive root modulo p. Removing row $p-1$ and column 1 from this construction leaves a Costas array of order $p-2$. When $g = 2$ is used as the primitive root mod p, the array can be further reduced to order $p-3$.

In Golomb's construction, if α and β are any two primitive elements in $GF(q)$, for $q > 2$, a Costas array of order $q-2$ is obtained by setting $a_{ij} = 1$ whenever $\alpha^i + \beta^j = 1$. (The case $\alpha = \beta$ had been discovered by A. Lempel.) If $\alpha + \beta = 1$, then $a_{11} = 1$, so that by removing row 1 and column 1, a Costas array of order $q-3$ is obtained. As shown in [6], for every $q > 2$, primitive roots α and β (not necessarily distinct) with $\alpha + \beta = 1$ can be found.

For $q = 4, 5, 9$, or any prime $p \equiv \pm 1 (\mathrm{mod}\ 10)$, and for no other finite fields, there is a primitive root α with $\alpha + \alpha^2 = 1$. Thus, in the Lempel construction, $a_{12} = a_{21} = 1$, so that if the first two rows and first two columns are removed, a (symmetric) Costas array of order $q-4$ results. For $q = 4, 5, 9$, or any prime $p \equiv 1$ or $9 (\mathrm{mod}\ 20)$, there are primitive roots α and β with $\alpha + \beta = 1$ and $\alpha^2 + \beta^{-1} = 1$. In this case, $a_{11} = 1$, $a_{2,q-2} = 1$, and $a_{q-2,2} = 1$. By successive removal of rows and columns, Costas arrays of orders $q-2$, $q-3$, $q-4$, and $q-5$ are obtained for these values of q. (See [5].)

In some cases, a Costas array of order $n+1$ can be obtained from one of order n by adjoining a 1 in an exterior corner, i. e. in one of the positions a_{00}, $a_{0,n+1}$, $a_{n+1,0}$, or $a_{n+1,n+1}$. Several prime order examples were obtained in this way from a Welch example of order $p-1$.

The total number $C(n)$ of Costas arrays of order n is known for $n \leq 23$ (see below), with a local maximum at $n = 16$.

n	$C(n)$	n	$C(n)$
2	2	13	12828
3	4	14	17252
4	12	15	19612
5	40	16	21104
6	116	17	18276
7	200	18	15096
8	444	19	10240
9	760	20	6464
10	2160	21	3536
11	4368	22	2052
12	7852	23	872

For prime p, there are $\phi(p-1)$ primitive roots, each of which leads to a different Costas array of order $p-1$. Since $\phi(p-1)$ can be arbitrary large, $\limsup_{n\to\infty} C(n) = \infty$. It has been conjectured but not proved that $\liminf_{n\to\infty} C(n) = 0$. This would require $C(n) = 0$ infinitely often. No case of $C(n) = 0$ is yet known, but no examples of Costas arrays of orders 32, 33, or 43 have yet been found. (Many larger orders also lack examples.)

John P. Costas first proposed these arrays for an application to frequency hopping sonar signals. Let the n rows represent n equally spaced frequencies, and the n columns, n equal duration time intervals. Then the Costas array specifies a permuted order for the n frequencies to be transmitted in n consecutive time intervals. As a sonar (or radar) signal, this design has an ideal, "thumb-tack" *ambiguity function* (the two-dimensional autocorrelation function in *time* and *frequency*). The horizontal (time) shift measures **range**, the *distance* to the target, and the vertical (frequency) shift measures **doppler**, the *velocity* of the target relative to the observer. For any non-zero shift parallel to the coordinate axes, a Costas array has at most one "hit" (coincidence of a 1 with a 1), and thus gives the least ambiguous reading of the correct range and doppler in the presence of noise.

BIBLIOGRAPHY

[1] Costas, J. P., *Project Medior — a medium-oriented approach to sonar signal processing*, HMED Tech. Publ. R66EMH12, General Electric Co., Syracuse, NY, 1966.

[2] Golomb, S. W. and Taylor, H., 'Two-dimensional synchronization patterns with minimum ambiguity,' *IEEE Trans. Inform. Theory* **28** (1982), 600-604.

[3] Golomb, S. W. and Taylor, H., 'Constructions and properties of Costas arrays,' *Proc. IEEE* **72** (1984), 1143-1163.

[4] Golomb, S. W., 'Algebraic constructions for Costas arrays,' *J. Comb. Theory (Series A)* **37** (1984), 13-21.

[5] Golomb, S. W., 'The T_4 and G_4 constructions for Costas arrays,' *IEEE Trans. Inform. Theory* **38** (1992), 1404-1406.

[6] Moreno, O. and Sotero, J., 'Computational approach to conjecture A of Golomb,' *Congressus Numerantium* **70** (1990), 7-16.

[7] Costas, J. P., 'A study of a class of detection waveforms having nearly ideal range-doppler ambiguity properties,' *Proc. IEEE* **72** (1984), 996-1009.

Note: This article on Costas Arrays, by S.W. Golomb, will appear in the **Kluwer Encyclopedia of Mathematics.**

B. *Zero-Sidelobe Radar*

The basic signal design problem for range radar is to find waveforms whose (normalized) autocorrelation function is unity "in phase", and close to zero "out-of-phase". For CW radars with phase modulation, many articles have been published describing imperfect and ad hoc techniques to construct such signals. However, in "Two-Valued Sequences With Perfect Periodic Autocorrelation" by S.W. Golomb, an infinite class of such waveforms, including arbitrarily long binary sequences as the modulating signals, is described, which achieve out-of-phase correlation *identically equal* to zero. A companion article by N. Levanon and A. Freedman shows that these signals are also highly favorable for range-doppler radar, having nearly ideal "ambiguity functions" (two-dimensional autocorrelation functions in both time and frequency). They assert that these new signals, derived from cyclic Hadamard difference sets, will be widely adopted in many important radar applications in the near future.

BIBLIOGRAPHY

[1] S.W. Golomb, "Two-Valued Sequences With Perfect Periodic Autocorrelation," *IEEE Transactions on Aerospace and Electronics Systems*, vol. 28, no. 2, April, 1992, pp. 383-386.

[2] N. Levanon and A. Freedman, "Periodic Ambiguity Functions of CW Signals With Perfect Periodic Autocorrelation", *IEEE Transactions on Aerospace and Electronics Systems*, vol. 28, no. 2, April, 1992, pp. 387-395.

C. *Generalized Barker Sequences*

Continuous-Wave (CW) Radars using a phase-modulated waveform have been in use for nearly fifty years. In 1953, R.H. Barker considered the question of finding the best *binary* sequences of phases, and found examples of sequences of lengths 2, 3, 4, 5, 7, 11, and 13. Unfortunately, no *longer* binary sequences exist. (This was *proved* in 1961 for *odd* lengths, and is universally *believed*, based on considerable evidence, for *even* lengths.) In 1965, Golomb and Scholtz introduced "generalized Barker sequences", which allow arbitrary finite sequences of phase angles $\{\phi_0, \phi_1, \ldots, \phi_n\}$, but with the "Barker constraint" on correlation:

$$|C(\tau)| \leq 1 \quad \text{for all } \tau,\ 1 \leq \tau \leq n,$$

where

$$C(\tau) = \sum_{k=0}^{n} a_k a^*_{k+\tau}, \quad a_k = e^{i\phi_k},\ a^*_k = e^{-i\phi_k}.$$

Gradually, longer and longer examples of these generalized Barker sequences (GBS) have been found, and in recent years, the list has been extended to all lengths ≤ 35, in a series of papers by Bömer, Antweiler, Friese, and Zottmann.

Among the GBS of the same length L, we define the *best* sequence to be the one for which

$$\max_{1 \leq \tau \leq L-2} |C(\tau)|$$

is minimized. For several values of L, we can describe the terms of the best sequence explicitly, and this work will be extended.

A very fruitful new idea has been to regard the sequence terms $\{a_0, a_1, \ldots, a_n\}$ as the coefficients of a polynomial,

$$f(z) = \sum_{k=0}^{n} a_k z^k,$$

$$\text{so that} \quad z^n f(z) f^*(1/z) = \sum_{k=0}^{2n} C(k-n) z^k,$$

and to consider the set of complex roots of $f(z) = 0$. The generators of the transformation group described in Golomb-Scholtz 1965 are easily interpreted in terms of their algebraic effect on $f(z)$, and in terms of their geometric effect on the set Λ of the roots of $f(z) = 0$. Symmetries of the GBS correspond directly to symmetries of the root set Λ.

It is anticipated that this collection of new methods will lead to the construction of bigger and better generalized Barker sequences for radar applications.

BIBLIOGRAPHY

1. R.H. Barker, "Group synchronization of binary digital systems", *Communication Theory* (Proceedings of the Second London Symposium on Information Theory), London, Butterworths, 1953, 273-287.

2. R. Turyn and J. Storer, "On Binary Sequences", *Proceedings of the American Mathematical Society*, vol. 12, no. 3, June, 1961, 394-399.

3. S.W. Golomb and R.A. Scholtz, "Generalized Barker Sequences", *IEEE Transactions on Information Theory*, vol. IT-11, no. 4, October, 1965, 533-537.

4. N. Zhang and S.W. Golomb, "Sixty-phase generalized Barker sequences", *IEEE Transactions on Information Theory*, vol. IT-35, no. 4, July, 1989, 911-912.

5. N. Zhang and S.W. Golomb, "Uniqueness of the generalized Barker sequence of length 6", *IEEE Transactions on Information Theory*, vol. IT-36, no. 5, September, 1990, pp. 1167-1170.

6. N. Zhang and S.W. Golomb, "Polyphase sequences with low autocorrelations", *IEEE Transactions on Information Theory*, vol. IT-36, no. 6, November, 1990, pp. 1478-1480.

7. N. Zhang and S.W. Golomb, "Polyphase sequences with low autocorrelations", *IEEE Transactions on Informations Theory*, vol. IT-39, no. 3, May, 1993, pp. 1085-1089.

8. L. Bömer and M. Antweiler, "Polyphase Barker sequences", *Electronic Letters*, vol. 25, no. 23, 1989, pp. 1577-1579.

9. M. Friese and H. Zottmann, "Polyphase Barker sequences up to length 31", *Electronic Letters*,vol. 30, no. 23, 1994, pp. 1930-1931.

10. M. Friese, "Polyphase Barker sequences up to length 36", *IEEE Transactions on Information Theory*, vol. IT-42, no. 4, July, 1996, pp. 1236-1238.

11. N. Chang and S.W. Golomb, "7200-phase generalized Barker sequences", *IEEE Transactions on Information Theory*, vol. IT-42, no. 4, July, 1996, pp. 1236-1238.

12. S.W. Golomb and M.Z. Win, "Recent results on polyphase sequences", submitted (1996) to the *IEEE Transactions on Information Theory*.

D. *Simplex Codes, and Cyclic Hadamard Difference Sets*

A *simplex code* is a collection of n real-valued signals $\{s_i(t)\}_{i=1}^{n}$ normalized to the unit interval, $0 \le t \le 1$, and to "unit energy" $\int_0^1 s_i^2(t)dt = 1$, such that the "simplex bound" on cross-correlation is achieved: $C_{ij} = \int_0^1 s_i(t)s_j(t)dt = -1/(n-1)$ for all $1 \le i < j \le n$. *Binary* simplex codes have $s_i(t) = \pm 1$ for all $i \in [1, n]$ and all $t \in [0, 1]$, and can be constructed if $n = 2a$ or $n = 4a$, where there is a Hadamard matrix of order $4a$. New examples of simplex codes, where the values of $s_i(t)$ are restricted (pre-normalization) to a small number of integers, are reported in [2].

A conjecture mentioned in [1] is that if there is a cyclic Hadamard difference set (i.e. a cyclic (v, k, λ) design with $v = 4a - 1, k = 2a - 1, \lambda = a - 1$) then v must be of one of three types: $v = 2^r - 1; v = 4a - 1 = \text{prime}; v = 4a - 1 = u(u + 2)$ where both u and $u + 2$ are primes. In [3], it is shown that all $v \le 10,000$, except for seventeen values not yet checked, satisfy this conjecture.

BIBLIOGRAPHY

[1] L.D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Mathematics #182, Springer-Verlag, Berlin, 1971.

[2] H.Y. Song and S.W. Golomb, "Some new constructions for simplex codes", *IEEE Transactions on Information Theory*, vol. IT-40, no. 2, March, 1994, pp. 504-507.

[3] H.Y. Song and S.W. Golomb, "On the existence of cyclic Hadamard difference sets, *IEEE Transactions on Information Theory*, vol. IT-40, no. 4, July, 1994, pp. 1266-1268.

E. *Legendre and Jacobi Sequences for Radar Applications*

The main constructions for the three classes of cyclic Hadamard difference sets mentioned in the previous section are: m-sequences for $v = 2^r - 1$; Legendre sequences (based on the Legendre symbol) for $v = 4a - 1 = \text{prime}$; and the "twin prime" construction (based on the Jacobi Symbol) for $v = u(u + 2)$ where u and $u + 2$ are both prime. All of these constructions are valuable as signal patterns for CW radar signals with ideal (two-level) periodic autocorrelation.

When the period is a prime of the form $p = 4a + 1$, no corresponding Hadamard difference set exists. However, if we define a periodic binary sequence by

$a_k = \begin{cases} (\frac{k}{p}), & \text{the Legendre symbol, for } 0 < k < p \\ 1, & k = 0 \end{cases}$, and cross-correlate it against

$b_k = \begin{cases} (\frac{k}{p}), & \text{the Legendre symbol, for } 0 < k < p \\ -1, & k = 0 \end{cases}$, we get a two-valued cross-correlation,

$C(\tau) = \begin{Bmatrix} \frac{p-2}{p}, & \tau \equiv 0 \pmod{p} \\ \frac{-1}{p}, & \tau \not\equiv 0 \pmod{p} \end{Bmatrix}$. This is proved in [1], by a method which generalizes from the Legendre symbol to the Jacobi symbol.

BIBLIOGRAPHY

[1] S.W. Golomb, with S. Gottesman and P.G. Grieve, "A class of pseudo-noise-like pulse compression codes, *IEEE Transactions on Aerospace and Electronics Systems*, vol. 28, no. 2, April 1992, pp. 355-361.

F. *Minimal Spanning Rulers*

The signal design problem of optimum spacing of the pulses in a pulse radar, or pulse sonar, system, leads to a combinatorial design problem referred to as the construction of *minimum spanning rulers* (also referred to in the literature as "optimum Golomb rulers"). A *spanning ruler* with n marks is a set of n non-negative intergers $0 = a_1 < a_2 < a_3 < \ldots < a_n = L$ (the n "marks on the ruler") such that all the $\binom{n}{2}$ differences $a_j - a_i$, $j > i$ (the "measured distances") are distinct. (This guarantees that the out-of-phase values of the unnormalized autocorrelation function never exceed 1.) The minimum L for the given value of n is the *length* of the minimum spanning ruler, and gives the shortest pulse pattern with the desired properties. This minimum $L = L(n)$ has now been determined for all $n \leq 19$.

Navy-related applications of these patterns include not only pulse-radar signals, but also sets of sequence delays for convolutional codes (a widely used form of forward-error-correcting coding), and linear spacing patterns for antennas for phased-array radars and for radio astronomy.

BIBLIOGRAPHY

[1] G. S. Bloom and S. W. Golomb, "Applications of numbered undirected graphs," *Proceedings of the IEEE*, vol. 65, no. 4, April, 1977, pp. 562-570.

[2] J. P. Robinson, "Optimal Golomb rulers," *IEEE Transactions on Computers*, vol. C-28, no. 12, December, 1979, pp. 943-944.

[3] E. J. Blum, F. Biraud, and J. C. Ribes, "On optimal synthetic linear arrays with applications to radioastronomy," *IEEE Transactions on Antennas and Propagation*, vol. AP-22, 1974, pp. 108-109.

[4] T. Kløve, "Bounds on the size of optimal difference triangle sets," *IEEE Transactions on Information Theory*, vol. IT-34, no. 2, March, 1988, pp. 355-361.

[5] T. Kløve, "Bounds and constructions for difference triangle sets," *IEEE Transactions on Information Theory*, vol. IT-35, no. 4, July, 1989, pp. 879-886.

[6] J. P. Shearer, "Some new optimum Golomb rulers," *IEEE Transactions on Information Theory*, vol. IT-36, no. 1, January, 1990, pp. 183-184.

[7] A. Dollos, T. Rankin, and D. McCracken, "Optimum Golomb rulers up to 19 marks," *IEEE Transactions on Information Theory*, to appear, 1996/1997.

G. *Other Areas Leading to Publications*

Examples of other recent technical publications by S. W. Golomb, listed below, are in the areas of 1) Probability and Information Theory, 2) Combinatorial number theory, 3) Ramsey theory, 4) de Bruijn sequences, and 5) Classification of Reed-Solomon codes.

[1] S. W. Golomb, "Probability, information theory, and prime number theory," *Discrete Mathematics*, vol. 106/107, September, 1992, pp. 219-229.

[2] S. W. Golomb, "An identity for $\binom{2n}{n}$," *American Mathematical Monthly*, vol. 99, no. 8, October, 1992, pp. 746-748.

[3] S. W. Golomb (with H.-Y. Song and H. Taylor), "Progressions in every two-coloration of Z_n," *Journal of Combinatorial Theory (Series A)*, vol. 61, no. 2, November, 1992, pp. 211-221.

[4] S. W. Golomb (with G. Mayhew), "Characterization of generators for modified de Bruijn sequences," *Advances in Applied Mathematics*, vol. 13, no. 4, December, 1992, pp. 454-461.

[5] S. W. Golomb (with I. S. Reed and H.-Y. Song), "On the non-periodic cyclic equivalence classes of RS codes," *IEEE Transactions on Information Theory*, vol. IT-39, no. 4, July, 1993, pp. 1431-1435.

II. *Technical Personnel Receiving Support During This Period*

Solomon W. Golomb, Professor, Principal Investigator
Herbert Taylor, Research Associate Professor
Hong-Yeop Song, Graduate Student and Post-Doctoral Fellow
Peter Gaal, Graduate Student

III. *Doctoral Research Completed*

A. *Theses Completed During This Period*

	NAME	*THESIS TITLE*	*COMPLETED*
1.	David Rutan	"Difference Sets and Analysis of the Periodic Correlation of Sequences," (now at Hughes Aircraft, El Segundo, CA)	1994
2.	C. Wayne Walker	"Solving the Error Locator Polynomial Over Finite Fields in Algebraic Decoding," (now at TRW, El Segundo, CA)	1993
3.	Hong-Yeop Song	"On Aspects of Tuscan Squares," (now at Yonsei University, Seoul, Korea)	1991

B. *Other recent doctoral graduates who have continued to collaborate in this research effort*

4.	Gregory Mayhew,	"Statistical Properties of Modified de Bruijn Sequences," (now at Hughes Aircraft, Fullerton, CA)	1988
5.	Gregory Yovanof,	"Homometric Structures," (now at Hewlett-Packard Research, Palo Alto, CA)	1988
6.	Ning Chang (né Zhang),	"N-Phase Barker Sequences," (now at Bell South, Atlanta, GA)	1988